IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

American Family Mutual Insurance Company,

Plaintiff,

-vs-

William W. Rickman,

Defendant.

Case No. 3:08 CV 583

MEMORANDUM OPINION AND ORDER

JUDGE JACK ZOUHARY

INTRODUCTION

This matter is before the Court on Defendant's Motion to Dismiss (Doc. No. 11). The matter has been fully briefed and a hearing was held on March 14, 2008.

Plaintiff American Family Mutual Insurance (AFI) employed Defendant William Rickman (Rickman) as an insurance agent from June 1998 until January 2008. Rickman began a relationship with Allstate Insurance (Allstate), a competitor of AFI, sometime in January or February 2008.

Plaintiff AFI alleges *inter alia* that Defendant Rickman violated 18 U.S.C. § 1030, also known as the Computer Fraud and Abuse Act (CFAA). The CFAA, primarily a criminal statute, also provides that: "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). This statute is the alleged basis for federal court jurisdiction (Compl. ¶ 3). Defendant challenges the application of this statute, and Plaintiff concedes,

if the statute does not apply, this Court must dismiss the action because all other claims arise from state law.[1]

ALLEGATIONS

Rickman was an agent for AFI from June 1, 1998 until his resignation effective January 31, 2008. During his employment he had access to confidential information and trade secrets (Comp. ¶ 6). The parties signed the American Family Agent Agreement (Employment Agreement) (Compl. Ex. A), which included language prohibiting Defendant, for one (1) year after his termination, from contacting customers to "cancel, replace or surrender" their policies. The Employment Agreement also required that Rickman, within ten (10) days of termination, deliver company property to AFI (Compl. ¶ 8).

Defendant was also "provided with access to the computer system and database" including confidential and trade secret information (Compl. ¶ 9). He agreed not to misuse this information pursuant to an Agent Automation Agreement (Compl. ¶ 10). While the Employment Agreement with AFI allows Rickman to access computer information, Plaintiff argues this authorized access is contingent on his being an agent and not working for a competitor. Plaintiff claims Rickman accessed customer and trade secret information "without authorization" or by "exceed[ing] authorized access"

---

[1] Plaintiff alleges four additional counts: (1) Breach of Contract; (2) Breach of Fiduciary Duties and Breach of Covenant of Good Faith for Fair Dealing; (3) Damages and Injunctive Relief under Ohio Revised Code § 1333.61; and (4) Punitive Damages. The Court's exercise of supplemental jurisdiction over these claims is discretionary under 28 U.S.C. § 1367(c)(3) once claims over which it has original jurisdiction are dismissed. Further, both parties are Ohio residents thereby defeating diversity jurisdiction.

in violation of the CFAA (Compl. ¶¶ 3, 21-24), and is using this information to benefit his new employer, Allstate.

Defendant's position is that even assuming "Plaintiff can prove the allegations as set forth in its complaint" (Motion to Dismiss at p. 5), because Rickman's initial computer access was permitted, his alleged conduct does not present an actionable matter under the CFAA and, further, the damages claimed by Plaintiff, namely lost profits, are not recoverable under the statute.

MOTION TO DISMISS STANDARD OF REVIEW

An action may be dismissed if the complaint fails to state a claim upon which relief can be granted. Federal Civil Rule 12(b)(6). The moving party has the burden of proving that no claim exists. Although a complaint is to be liberally construed, it is still necessary that the complaint contain more than bare assertions or legal conclusions. *In re DeLorean Motor Co.*, 991 F.2d 1236, 1240 (6th Cir. 1993) (citing *Scheid v. Fanny Farmer Candy Shops, Inc.*, 859 F.2d 434, 436 (6th Cir. 1988)). All factual allegations in the complaint must be presumed to be true, and reasonable inferences must be made in favor of the non-moving party. 2 MOORE'S FEDERAL PRACTICE, § 12.34[1][b] (Matthew Bender 3d ed. 2003). The Court need not, however, accept unwarranted factual inferences. *Morgan v. Church's Fried Chicken*, 829 F.2d 10, 12 (6th Cir. 1987). To survive a motion to dismiss, the complaint must present "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, ____ U.S. ____, 127 S.Ct. 1955, 1974 (2007).

DISCUSSION

Unauthorized Access

The initial inquiry for this Court is whether the CFAA can be used against employees who access information from a company computer and later use that information against the employer.

To answer that question, the Court starts with a review of the statutory language that defines a violation of the CFAA:

> (4) [A person violates the CFAA if he or she] knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

§ 1030(a)(4).

AFI alleges Defendant exceeded his authorized access, defined in the statute as follows:

> [T]he term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.

§ 1030(e)(6).

Defendant argues this definition does not apply to his conduct because he did not obtain any information to which he was not entitled nor did he alter any information. Plaintiff concedes no information was altered but argues Defendant was not authorized to utilize this information against AFI in violation of his employment agreements. The employment agreements between AFI and Defendant do not limit his use of the computer system, and there is no definition of confidential or trade secret information. Plaintiff is essentially complaining about the **use** of properly accessed information. Rickman was authorized to initially access the computer and was permitted to review the files, but allegedly he later misused that information by sharing it with Allstate.

Another court which had occasion to discuss this very issue is *Brett Senior & Assocs. v. Fitzgerald*, No. 06-1412, 2007 WL 2043377 (E.D. Pa. July 13, 2007). In that case, defendant, while in discussion with a competitor about potential employment, created a list of clients which he showed to his potential new employer. He later joined the competitor. There was no dispute defendant

exceeded his authority when he e-mailed documents considered proprietary. The court there reasoned:

> In other words, did Fitzgerald access a computer "without authorization" or "exceed[ ]" his "authorized access"? The plaintiff argues that the latter phrase is applicable, but the text of the statute, the rule of lenity, and legislative history show otherwise.
>
> The CFAA defines "exceeds authorized access" as accessing "a computer with authorization" and using "such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* § 1030(e)(6). By its plain terms, this definition does not apply to Fitzgerald's conduct. He did not obtain any information that he was not entitled to obtain or alter any information that he was not entitled to alter. As Senior testified at his deposition, Fitzgerald was allowed full access to information contained in the BSA computer system until his departure.

Id. at *3.

Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008), addressed a similar situation and reached a similar conclusion. There, an employer brought a complaint under the CFAA against a former employee and a competitor; defendants moved to dismiss. The court held that an employee's access to confidential information **prior** to his resignation did **not** give rise to a cause of action under the CFAA. First, the court noted the plain language of the statute which, according to *Fitzgerald,* targeted "the unauthorized procurement or alteration of information, not its misuse or misappropriation." *Shamrock*, 535 F. Supp. 2d at 965 (citing *Fitzgerald*, 2007 WL 2043377, at *3). Second, the court noted the legislative history supported "a narrow view of the CFAA" and that the general purpose "was to create a cause of action against computer hackers (e.g., electronic trespassers)." *Id.* at 966 (citations omitted). The court further noted the legislative history in support of a narrow reading of the statute:

> The 1984 House Committee emphasized that "Section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer . . . in committing the offense. . . . Consequently, the committee report emphasized concerns about "hackers" who "trespass into" computers and the inability of "password codes" to protect against this threat.

Id. at 965 (citations omitted).

The *Shamrock* court concluded, given the plain language of the statute, legislative history, and principles of statutory construction, a restrictive view of "authorization" was appropriate and a violation for accessing "without authorization" occurs only where initial access is not permitted. The *Shamrock* court also concluded a violation for "exceeding authorized access" occurs where initial access is permitted but the access of certain information is prohibited. Because defendant was authorized to access the computer and view the files, the court found plaintiff failed to state a CFAA claim and refused to exercise supplemental jurisdiction over the state law claims, thereby dismissing the case. *Id.* at 968.

One court has described the difference between "without authorization" and "exceeding authorized access" as "paper thin but not quite invisible." *Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006). In *Citrin*, the allegation was that the employee had violated his duty of loyalty by destroying data in a breach of an employment agreement. When defendant left his employer, he returned his computer but allegedly erased files. The court there found sufficient allegations for the CFAA claim to withstand a motion to dismiss, focusing on the alleged violation of duty of loyalty and agreement "not to disseminate confidential data after he left the company's employ." *Id.* at 421; *see also Int'l Sec. Mgmt. Group v. Sawyer*, No. 3:06 CV 0456, 2006 WL 1638537, at *20-21 (M.D. Tenn. June 6, 2006) (e-mailing documents to competitor was sufficient to sustain CFAA claim).

Other courts broaden the scope of the CFAA to include a breach of confidentiality agreements, employment agreements, or company policies on computer use. *Hewlett-Packard Co. v. Byd: Sign, Inc.*, No. 6:05-CV-456, 2007 WL 275476 (E.D. Tex. Jan. 25, 2007) summarized this split of authority as follows:

> Several courts have concluded that an employee may exceed his authorization or may act without authorization when he obtains proprietary information from his employer's computers and uses that information in a competing venture. *See International Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) (reversing dismissal of CFAA claims where employee went into business for himself and used "scrubbing" software to delete all of the files on his company-issued computer); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-84 (1st Cir. 2001) (finding that employer was likely to prove access in excess of authorization where former employee obtained proprietary information and then provided that information to his new employer in violation of his confidentiality agreement.); *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (finding that the employee acted without authorization when he obtained proprietary information from his former employer's computers for the benefit of his new employer.).
>
> [S]everal courts have questioned the key holdings in the above cited cases. *See, e.g., Lockheed Martin Corp. v. Speed*, 2006 U.S. Dist. Lexis 53108, at *12, *16-*25 (M.D. Fla. August 1, 2006); *Int'l Assoc. of Machinists and Aerospace Workers v. Werner-Matsuda*, 390 F. Supp.2d 479, 499 D. Md. 2005); *Secureinfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 609-10 (E.D. Va. 2005).
>
> * * *
>
> As stated by the court in *Werner-Matsuda*, "the gravamen of [the plaintiff's] complaint is not so much that [the defendant] improperly accessed the information …, but rather what she did with the information once she obtained it." 390 F. Supp. 2d at 499.

Id. at *12-13.

The gravamen here, too, is what Defendant did with allegedly proprietary information. However, the Court need not resolve this split of authority because its analysis of "loss" under the CFAA provides a clear basis for dismissal. The Court turns to the statutory definition of "damage" and "loss" as well as case law interpreting these statutory definitions.

Revenue Lost

The applicable civil remedy provision of the CFAA requires an allegation of "loss" of at least $5,000. 18 U.S.C. § 1030(g), (a)(5)(B)(i) ("loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value").

The CFAA defines "damage," "loss" and available relief as follows:

> (8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;
>
> * * *
>
> (11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;
>
> * * *
>
> (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.

18 U.S.C. § 1030(e)(8), (e)(11), (g).

Plaintiff AFI conceded at oral argument that Subsection 8 does not apply and that Plaintiff is basing its claim on the phrase "any revenue lost" in Subsection 11 (Tr. 17-18). Plaintiff interprets those words broadly while Defendant argues they are limited by the remainder of the phrase which places "revenue lost" in the context of computer hacking ("interruption of service"). When Subsection 11 is read in its entirety, as it must be according to the principles of statutory construction, "any revenue lost" cannot provide the broad scope that Plaintiff suggests. Rather, "revenue lost" is read in conjunction with the rest of the phrase: "and any revenue lost, cost incurred, or other consequential damages incurred **because of interruption of service**" (emphasis added). The statute

was not meant to cover the disloyal employee who walks off with confidential information. Rather, the statutory purpose is to punish trespassers and hackers; Defendant is neither.

In *Lockheed Martin Corp. v. Speed*, No. 6:05-cv-1580-orl-31KRS, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006), plaintiff, an aerospace government contractor, alleged defendant, a former employee, copied proprietary information and delivered trade secrets to a defendant rival in violation of the CFAA. The court reviewed the complaint on a motion to dismiss and focused on the statute's private cause of action which requires that a plaintiff "suffer a root injury of damage or loss." *Id.* at *3. In *Lockheed*, as in the instant case, the primary injury was the communication of trade secrets or sensitive information to a competitor. The court found plaintiff was not entitled to relief under the statute because the employee's computer access was permitted and because plaintiff did not meet the statutory definition of permissible damages. *Id.* at *8.

The opposite result was reached in *Hewlett-Packard, supra*, where the court declined to dismiss an employer's claims against former employees for passing along trade secrets and other proprietary information. However, in *Hewlett-Packard*, the defendant employees each signed a confidentiality agreement which was the crux of the complaint. The court acknowledged the different lines of authority and concluded plaintiff had alleged access "without or in excess of authorization" because the employment and confidentiality agreements compelled defendants "not only to refrain from disclosing information, but also to refrain from sending or accessing messages on HP's computer systems for personal gain."[2] Plaintiff points to *Sawyer*, *supra*, as a case with similar damages. However, the *Sawyer* court did not address loss or damage squarely. Indeed, the CFAA claim there

---

[2] There was also a charge in that case that defendants "scrubbed" their computers thereby damaging or deleting HP information. This latter act would clearly fall within the scope of Section 1030(a)(5). *Id.*

was merely ancillary to the state law claims and received only brief treatment as an alternative or additional grounds for relief. 2006 WL 1638537, at *20-21.

Recently, *Modis, Inc. v. Bardelli*, 531 F. Supp. 2d 314 (D. Conn. 2008), addressed a motion to dismiss under the CFAA. In that case, while still employed by plaintiff, defendant began communicating with representatives of a competitor concerning potential employment. After she left Modis, defendant was hired by the competitor. Plaintiff alleged defendant divulged confidential trade secrets and other proprietary information during the course of her employment at Modis. The court noted the split in authority on whether defendant had "exceeded authorized access," but bypassed that issue by focusing on the damage or loss sections of the statute. *Id.* at 319. Defendant submitted that recoverable losses under the CFAA are limited to the cost of analyzing or restoring the computer information and revenue lost "because of interruption of service." The court found plaintiff's claims of damages insufficient to meet the statutory definition and granted the motion to dismiss the CFAA claim (although allowing plaintiff an opportunity to re-plead to amplify the grounds for asserted relief, including "the costs of responding to the offense"). *Id.* at 320.

This plain reading of permissible damages under the statute is echoed in *L-3 Commc'ns Westwood Corp. v. Robicharux*, No. 06-0279, 2007 WL 756528 (E.D. La. Mar. 8, 2007), where the court denied a request for a preliminary injunction. The court found that allegations of loss of trade secrets and lost profits are not contemplated by the CFAA:

> The meaning of 'Loss' both before and after the term was defined by statute, has consistently meant a cost of investigating or remedying damage to a computer or a cost incurred because the computer's service was interrupted.

Id. at *3 (quoting *Nexans Wires, S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 475 (S.D.N.Y. 2004), *aff'd* 166 F. App'x. 559 (2006)). Losses are "compensable when they result from damage to a computer system or the inoperability of the accessed system." *Id.* at *4.

Likewise, in *Nexans*, the case upon which the *Robicharux* court relied, the court concluded "revenue lost because the information was used by the defendant to unfairly compete after extraction from a computer does not appear to be the type of 'loss' contemplated by the statute." 319 F. Supp. 2d at 478. The *Nexans* court determined it is insufficient to "claim[ ] to have lost money . . . because of the way the information was later used." *Id.* at 477. The CFAA does not contemplate consequential damages such as lost business or profits that are unrelated to harm to the computer itself.

What is clear from all these cases is that indirect damages are recoverable, but there must be an underlying intrusion into the computer system or computer data and that "loss" was intended to "target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker." *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001). Indeed, the underlying premise of this criminal statute is directed toward computer piracy, and the loss of revenue must be related to the misuse of the computer -- something more than misuse of information obtained from the computer through authorized access. The Defendant in the instant case, Rickman, may have violated his employment agreements, but the allegations against him are not that he was a computer pirate or that he otherwise caused harm to AFI's computer.

CONCLUSION

The damages sought by Plaintiff AFI are exactly the type of damages sought by plaintiff in *Robicharux*. Plaintiff's expansive reading of "any revenues lost" would make the statute applicable to every employee who allegedly violated an agreement with the employer. That is not the purpose of the statute. Rather, the statute is limited to the destruction and/or damage of computer information. Prior to the widespread use of computers, an employee could walk off with confidential paperwork; with computers, the employee can walk off with the disc, or quietly transmit the information to an outside source. This method is easier than trying to hide the paperwork in a bulging sack or expandable briefcase, but computer access alone does not make the conduct subject to the CFAA. An employer still has traditional state statute and common law remedies available to it for recovery against the dishonest employee.

The Complaint, on its face, does not satisfy the requirements of the CFAA. Plaintiff has not alleged the type of loss which comes within the scope of the statute. Therefore, since this is the only basis for federal court jurisdiction, the Court dismisses this action without prejudice.

IT IS SO ORDERED.

s/ *Jack Zouhary*
JACK ZOUHARY
U. S. DISTRICT JUDGE

April 18, 2008